Avionics/Intelligence and Electronic Warfare Bulletin

(Formerly the "ARAT Bulletin")

"Serving the Needs of the Army's A/IEW Community"

Volume 1, Issue 1 **April 2000**

The New Millennium Brings Changes to Names, But Not to Warfighter Support

Happy New Millennium! In January, many of you received your "ARAT Bulletin" from the Army Reprogramming Analysis Team (ARAT)- Project Office. You are probably wondering why you are now receiving the "Avionics/Intelligence and Electronic Warfare Bulletin" from the Army's Communications-Electronic Command's Software Engineering Center (CECOM SEC).

The ARAT-PO officially ceased to exist at the end of Fiscal Year 1999. However, due to the hard work, planning and implementations executed during the ARAT-PO's six-year history, the core ARAT services remain in place to support Warfighters who must reprogram their ATSS to remain fully operational. The services formally provided by the ARAT-PO, such as communications infrastructure support in the form of establishing ARAT services, servicing users' accounts, troubleshooting connectivity problems, and providing guidance on system requirements and configuration have transitioned to the CECOM SEC Electronic Combat Branch (ECB). This change is transparent as the ARAT-PO, although funded by HQDA through the Land Information Warfare Activity (LIWA), had always resided within the ECB.

In This Issue

As for the rest of the ARAT, nothing has changed. The ARAT-Threat Analysis Center at Eglin AFB will continue to provide timely threat analysis and work to ensure that the most current information is programmed into all Mission Data Sets (MDSs). The ARAT- Software Engineering Center, staffed by members of the SEC ECB, will continue to develop MDSs for Aviation self-protection systems such as the AN/APR-39(V)2, -39(A)V1, and –39A(V)2. Additionally, the ARAT- Support Cell at Fort Rucker will continue to address doctrinal issues that complement the threat analysis and MDS to form a complete system of Aviation protection.

Bottom line: the ARAT still exists! The ARAT always has and will continue to be "a networked group of activities working together to support Warfighters and their sophisticated target sensing systems". The members of the team will keep on maintaining the products and services they have developed and incorporate new and evolving technology in a concerted effort to counter threat systems on the battlefield- anytime, anywhere.

Written by the "A/IEW Bulletin" Staff

The "Avionics/Intelligence and Electronic Warfare Bulletin" is a quarterly professional periodical published by the CECOM SEC Avionics/Intelligence and Electronic Warfare Division

From the Senior Editor's Desk

Written by Mr. Joseph Ingrao, Deputy Chief (A)

Major Changes with Small Steps

The most effective change processes are incremental. They break down big problems into small, doable steps. The key essential of creating positive change within a system or a team is mobilizing for fast actions and sustaining commitment.

Some small changes are taking place to expand the "ARAT Bulletin" to encompass the Avionics, Intelligence and Electronic Warfare (A/IEW) systems. You will be seeing articles from six of the US Army's premier software and system sustainment branches:

- **Guardrail Branch**
- **Electronic Combat Branch**
- **Sensors Branch**
- **Avionics Branch**
- **Intelligence Fusion Branch**
- **SIGINT / Surveillance Branch**

The inclusion of this team information will provide us with new and different views of systems and software that ultimately all work together to support our Warfighters. The key points of contact for each branch are provided in this bulletin, and they look forward to answering all pertinent questions you may have in supporting your systems.

Here at the CECOM SEC A/IEW Division we have embraced the strategy of major changes through small victories. We have taken steps to ensure that the engineers in our labs can take fast and responsive actions. They are encouraged to experiment continuously and always reduce systems to their essence. The magic in achieving small victories is the experimentation process, setting up tests that continually help in understanding what future capability the system may have.

It has been and always shall be our commitment to provide and sustain the best-engineered systems to support and protect the soldiers in the field.

Software Engineering Center's GUARDRAIL Branch– Year 2000

From battling Y2K bugs to marshalling millions of lines of legacy systems' code, the CECOM Software Engineering Center (SEC) is perpetually reinventing itself to meet the software system needs of today's Army. A prime example is the large and intricate GUARDRAIL (GR) family of systems administered and supported by SEC's GR Branch within the A/IEW Division. The GR Team has been in operation since the 1980s and has continuously demonstrated a high degree of:

- Technical competency and accomplishments;
- Efficient system operations;
- Cost benefits;
- Efficient resource management including budget(s), schedules, personnel allocation and contractor performance oversight;
- And, the bottom-line: *customer satisfaction*.

In addition, SEC has successfully migrated to emerging DoD/Army acquisition strategies, management tools and techniques, and technical thrusts.

Meeting Customer Needs

To meet the needs of the soldiers in the field and its PM customers, SEC functional areas, such as the GR Branch, are constantly extending, modifying and upgrading capabilities and resources to meet high priority challenges such as continuous and timely field support, new tasking, emergencies, and field anomalies. For example, the GR Branch responds to these challenges with the following positive actions regarding capabilities and resources in various areas:

Acquisition

- Staying aware of the changing battlefield and Army mission;
- Using acquisition streamlining tools/techniques, e.g., paperless solicitation process, open acquisition process to share information/ideas/understanding; integrated procurement team approach, etc.
- Utilizing DoD-mandated increased contractor lifecycle support;
- Leveraging Operations & Support Cost Reduction (OSCR), Total Ownership Cost Reduction (TOCR), and Product Improvement Program (PIP) cost savings where applicable;
- Cooperating with other Army and non-Army agencies.

Management

- Accomplishing quality up-front planning;
- Initiating project oversight on a regular basis through use of metrics, configuration management (CM), project databases; status/milestone/progress reporting & reviews, test & quality assurance (QA) procedures & functions; etc.;
- Implementing improved government-contractor support team communications and interfaces including: electronic media; ad-hoc and case-by-case meetings/discussions timely/quick responses; continuous discussions aimed at viable solution paths; etc.

(Cont. Page 12)

Intelligence Fusion

Intelligence Fusion Systems Partnership in Sustaining Military Intelligence Information Systems Software

Introduction

The U.S Army CECOM SEC, Intelligence Fusion Systems Branch (IFS), is a prominent partner with the Intelligence Community for software engineering services. SEC IFS has achieved phenomenal success and continues to earn the trust and respect of the warfighting army by handling the U.S. Army's challenges with innovation and excellence. SEC IFS provides comprehensive customer-focused solutions and tailored software engineering services. SEC IFS is responsible for supporting the MI Community and ensuring that tactical automation used in support of intelligence analysis is the best in the world.

Overview

The SEC IFS is a recognized Department of Defense (DoD) leader in software, maintenance, enhancement, integration, and Field Software Services Support (FSSS). During the past four years, in conjunction with its prime contractor, ILEX Systems, SEC IFS has developed software modifications and enhancements and has tested, documented, and provided configuration management for 43 versions of the U.S. Army All Source Analysis System (ASAS), Digital Topographic Support System (DTSS), and Integrated Meteorological System (IMETS) software.

In response to reports of soldier needs, the new baselines included enhancements such as "point and click" interfaces, a Modernized Intelligence Database (MIDB) 2.0 functionally scheduled for implementation in the First Digitized Division Analysis and Control Element (FDD ACE), and up to a six-fold increase of message processing speeds. SEC IFS upgraded and tested all Intelligence Fusion systems for Y2K compliance and certified these ASAS systems in every Army Theatre through successful Operational Evaluations.

Team ASAS includes SEC IFS, the ASAS Project Manager, the TRADOC System Manager ASAS, and the partnering prime contractor, ILEX Systems. Responding to U.S. Army requirements for expanded capabilities in the ASAS, SEC IFS routinely develops software for incremental releases to field units. Since 1994, SEC IFS has transitioned six complex Intelligence Fusion and Terrain/Weather systems from development contractors to a comprehensive Post Production Software Support (PPSS) environment.

Professional Staff

SEC IFS professional staff consists of more than 300 personnel experienced in Software Development, Testing, Quality Assurance, and Configuration Management. The technical staff is proficient in Open-Virtual Memory System (VMS) and Solaris Operating Systems (OS), Oracle and Informix Database Management Systems (DBMS), C, C++, Pascal, FORTRAN, Ada, and 11 distinct scripting languages. The SEC IFS and FSSS staffs represent hundreds of man-years of software development and on-site support experience.

(cont. next page)

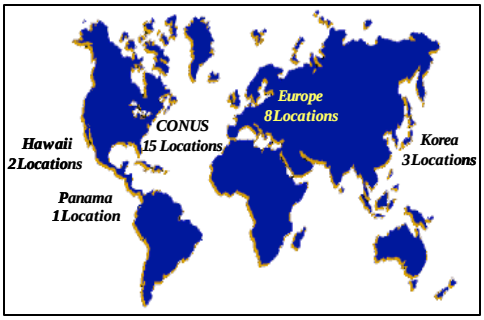
Intelligence Fusion *(cont.)*

Department of Defense Support

SEC IFS supports over 1,500 Army IFS and Terrain/Weather workstations fielded worldwide, serving field commanders from Brigade to Joint Service level. SEC IFS manages and staffs the CECOM Intelligence and Electronic Warfare Integration Laboratory, which provides the latest versions of fielded ASAS software for interoperability testing with other U.S. Army systems. Integral to the test element, SEC IFS has an extensive security engineering section responsible for security testing, providing documentation for accreditation and certification, tracking and adhering to all security-related bulletins, and investigating available C2 Protect tools.

Worldwide Field Support

The SEC IFS FSSS is widely recognized within the U.S. Army intelligence community for its excellence in the area of on-site field support. An Operations Center coordinates the activities of seven global regions.



The seven regions, resident with each Corps Headquarters, U.S. Forces Korea, and the U.S. Army Intelligence Center, direct the support activities of over 150 field software engineers in 10 countries. Annually, FSSS engineers support over 100 exercises ranging from Brigade to Joint and Combined readiness exercises.

FSSS engineers support the total U.S. Army to include Army Reserve and National Guard units. Annually, SEC IFS engineers conduct over 45 support visits to National Guard and Army Reserve units.

Last year, FSSS technicians supported 18 Army technical tests initiatives, provided support to over 213 military events/exercises, and deployed 21 personnel for operations in Bosnia, Kosovo, and Kuwait. Our deployable Tiger Team is ready to solve specific unit problems between semi-annual software upgrades. Critical to our success is a well-defined configuration management process, which ensures that deploying units have the latest software versions and remain interoperable worldwide.

SEC IFS will continue to develop its expertise on joint intelligence systems. SEC IFS will continue to serve as a center for excellence, providing technical expertise on fielded intelligence software and on the new and emerging technologies associated with intelligence systems, information systems, and automation. Through its ability to manage intelligence fusion systems processes, SEC IFS will continue to be a Premium Partner to the MI Community.

For further information, or to obtain SEC IFS services and solutions, contact us at the address below.

United States Army Communications-Electronics Command
Software Engineering Center Intelligence Fusion Systems
Fort Huachuca, Arizona 85613-5000
Phone (520) 538-6188; DSN 879-6188
http://cecom-ifs.army.mil

Written by Mr. William R. Walker, CECOM SEC IFS

The Future of Heads Up Displays

Software Engineering Center Assumes New Software Maintenance Role

The United States Army CECOM SEC recently assumed the duties and responsibilities to maintain software for the Advanced Aviator's Night Vision Imaging System/Heads Up Display (AHUD).

AHUD was developed to improve combat and assault military helicopter operations and survivability on the modern battlefield. It collects and displays critical flight information from aircraft sensors and converts it into visual imagery. The system allows continuous "heads-up" flight without the need to continuously look down at the cockpit instrument panel.

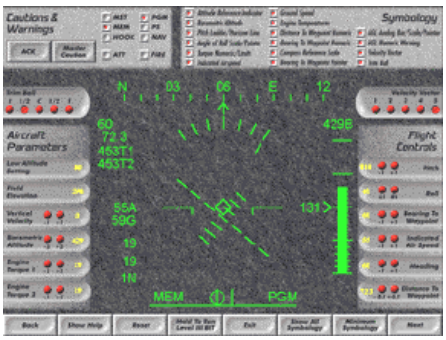
The AHUD is an Advanced Electro-Optical System integrated with the Night Vision Goggle (NVG). The system senses critical flight data (i.e., altitude, airspeed, attitude, torque, compass heading) and transmits the data to the NVG. The data is overlaid on the NVG imagery to provide the pilot and copilot with integrated night scene and critical flight data symbology. This results in significant operational advantages and survivability enhancements when performing night missions.

Software Engineering Center (SEC)

SEC has the United States Army responsibility for performing Life Cycle Software Engineering Support (LCSES) for all computer-based battlefield systems. LCSES is the overall system support necessary to develop, sustain, modify, refine and improve software for the computer-based battlefield systems, including computer code, databases, documentation and other support software and hardware components.

AHUD LCSES

The AHUD Program Manager, from CECOM Night Vision Electronic Sensors Division appointed SEC with the new role to provide LCSES for the AHUD Program. This role requires SEC to transition AHUD software from the developer, review and maintain software documentation, develop, sustain, modify, refine and improve AHUD software; and perform Engineering Change Proposal evaluation.



Sample AHUD Display through NVG

Successful AHUD LCSES performance will require SEC to establish an AHUD Software Maintenance Facility at Fort Monmouth, New Jersey. This facility will provide SEC the ability to perform software development, modification, refinement, troubleshooting, diagnostics and testing of software with an Aircraft Interface Simulator test stand. The facility will be operational during Spring 2000.

(cont. next page)

Heads Up Displays *(cont.)*

During Year 2000, SEC will provide AHUD LCSES for software transition from the developer, and software modification to support the CH-47D Chinook engine variant, and integration for the UH-60Q MEDEVAC BLACKHAWK glass cockpit integration.

The AHUD software modifications will require SEC to perform engineering analysis of aircraft sensors, sensor indicator metrics, parameters and ranges to determine their impact to the flight information delivered to the AHUD processor; and computer code analysis to evaluate flight information conversion. Software refinement or modification and software testing at the SEC AHUD Software Maintenance Facility will follow the analysis and evaluation.

Written by Mr.Kwok Lo, CECOM SEC

Training Update

ARAT MDS Training Product for the AN/APR-39A(V)1

The CECOM SEC Electronic Combat Branch (ECB), along with its support contractor SRI, International, has completed an unclassified Mission Data Set (MDS) training product for the AN/APR-39A(V)1. Rich in multimedia content, this product is being distributed on CD-ROM and is viewable on any IBM-PC compatible system. This training product is tailored to a generic MDS, and includes emitter and threat type information, as well as display representations, relative to the AN/APR-39(V)1 Radar Signal Detection Set.

The training is accomplished via a mixture of text, graphics, pictures, animations, video, and audio. Considerable user interaction is available on almost every topic to promote a better understanding of the AN/APR-39A(V)1 capabilities and Electronic Warfare in general. The table of contents is shown below.

This training product will be distributed to students of the EWO training course taught at Fort Rucker when they have completed the course. In addition, EWOs can request this multimedia product by contacting Mr. Gary Clerie, ECB Chief, at DSN: 992-0065.

ASE Anomalies

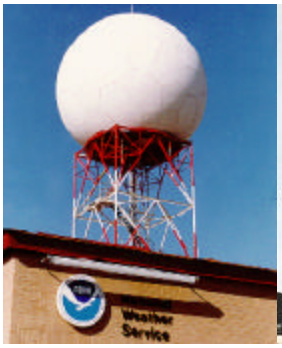
'Pulses to the right of me, pulses to the left of me…'

It sure is a complicated and busy world out there. When we drive home from work, we wonder why it takes us so long because of all those other drivers on our same route. When we are on vacation flying to our destination, we wonder why we don't arrive on time because of all those other airplanes trying to land at the same time. It is much the same with the Aircraft Survivability Equipment (ASE) we have installed on our aircraft and the environments in which we require them to try and effectively operate 100% of the time. We not only have to worry about how our systems detect and display the 'real' emitters, but also how our systems try to define and refine them while being bombarded by all those other electrons floating around in our dense domestic and foreign communication environments.

On one side of the equation we have radar systems that we might consider 'threat' radars operating over a very wide Radio Frequency (RF) range. As an example, open source literature details the Russian Knife Rest Early Warning (EW) radar operating from 70-73 MHz [(1)], the Casta-2E1 EW radar in UHF band [(2)], Fire Can from 2700-2900 MHz [(3)], Jay Bird Airborne Radar from 12.88 to 13.2 GHZ [(4)], and Gun Dish from 14.6-15.6 GHZ [(5)]. Each one of these, because of its function, has a radar fingerprint that may enable them to work in many different regimes, e.g. clutter, jamming, low altitude, or long range. Naturally there are many, many more emitters within and outside these frequencies with similar or greater capabilities that our aviators are exposed to.

Specific units within the U.S. Army are on extremely short alerts to be able to deploy anywhere in the world. Consequently the ASE that is carried on Army aircraft supporting those units have to be prepared, i.e., programmed and tested with emitters that reflect all the possible contingencies and locations of operation.

Because of weapon and radar proliferation there are many weapon-associated radars deployed throughout the world that our aviators may encounter. Sophisticated systems manufactured by France (e.g., Crotale operating in E and J bands [(6)], Crotale NG operating in S and Ku bands [(7)]); Sweden (e.g., Giraffe operating in G/H bands [(8)]), the United Kingdom (e.g., Rapier operating in E and K bands [(9)]), Switzerland (e.g., Superfledermaus operating in I band [(10)]), the Netherlands (e.g., Flycatcher operating from 8500-9600 MHz and approximately 34 GHZ [(11)]), and the US (e.g., Patriot operating in G band [(12)]), have all been added to the inventories of many countries. All these radiate at various RFs and with pulse modulations that may cover the spectrum from simple to complex e.g., constant, stagger and jitter.



(cont. next page)

ASE Anomalies *(cont.)*

It might seem easy that our ASE would always perform effectively 100% of the time with just these types of weapon related radars in our operating environment. But our equation is incomplete. We now must consider a multiplicity of commercial radio, television, microwave, VHF, HF and UHF transmissions. Pilots using our ASE installed on AH-64s, OH-58s, CH-47s, H-60s, RC-12s, RC-7s, C-130s at many of our facilities in the US and forward deployed locations are additionally tracked, monitored and painted by emissions from such systems as Approach Surveillance Radar (ASR) (e.g., ASR-9 operating from 2700-2900 MHz [13]), Precision Approach Radar (PAR) (e.g., AN/FPN-40 operating from 9000-9160 MHz [14]), weather radar (e.g., NEXRAD operating from 2.7-3.0 GHz [15]), AWACS (e.g., AN/APY-1 operating in F band [16]), Airborne Intercept (e.g., AN/APG-66 operating in I/J bands [17]), counter-mortar radar, (e.g. Cymbeline operating in I band [18], AN/TPQ-36 operating in I band [19]), low altitude/ force protection radar (e.g., AN/MPQ-64 operating in X Band [20]), long range naval EW and surface search radars (e.g., AN/SPS-48 operating from 2900-3100 MHz [21], AN/SPS-67 operating from 5450-5825 MHz [22]), on-board terrain-following and weather radars (e.g., AN/APN-241 operating from 9300-9410 MHz [23]) and fire control radars (e.g., AN/APG-78 operating in millimeter band [24]).

Taking into account the capabilities and limitations of all the different types of installed ASE and the simple to complex pulse environment in which our aircrews fly, it is easy to deduct that anomalies may occur in detection and identification.

To try and identify, quantify and alleviate possible anomalies, CECOM SEC ECB and ARAT-TA have placed an unclassified anomaly worksheet on the Multi Service Electronic Warfare Bulletin Board System (the BBS) that can be downloaded and used to record specific data that can possibly be used to reconstruct a snapshot of the pulse environment and the operation of the ASE. Using data from the aircrew and supporting data available from other sources, CECOM and the ARAT-TA may be able to determine why the ASE acted in the specific way it did. ARAT-TA has access to extensive collection asset data and CECOM has the capability to generate emitters on sophisticated simulators that are hooked to the respective ASE. Trying to specify possible anomalies can be important because it can improve preflight planning, mission profile and confidence in the fielded ASE.

The anomaly worksheet is found in the "AN/APR-39A(V)1" Library but the information outlined on the sheet has applicability to other ASE. The anomaly sheet is unclassified until it is filled in – then it becomes

(cont. next page)

classified. The data that we ask for covers the full spectrum: type of aircraft; single or multiple platforms;

ASE Anomalies (cont.)

location and time of anomaly (e.g., home base or deployed); installed and operative ASE; OFP and MDS loaded, known local emitters close to the anomaly (e.g., ASR, PAR, Patriot, TPQ-36); anomaly symbol description and movement on the display; and correlation with other platforms if possible.

When the sheet is completed it can be sent back to CECOM or the ARAT-TA via the MSEWBBS or faxed to our secure fax numbers. ARAT-TA's secure fax number is 850-882-9609 or DSN 872-9609. If you can't get to the BBS give us a call on a STU III at 850-882-8899 or DSN: 872-8899 and we can collect the information verbally.

We don't want to say we can answer all reported anomalies immediately. It may take us some time to pull all the supporting documentation together to make an informed reply. CECOM and ARAT-TA give priority to anomalies reported by the deployed units and then US based units. Experience has shown us that detailed reporting on an anomaly, coupled with signature data collection and in-depth simulator testing, can and does make a difference to the manner in which the ASE is programmed. As a result, the way the ASE detects and identifies an emitter may be improved. In a follow-on article we want to bring you a real world example where input from field users resulted in the implementation of changes to programming and improvements to detection and identification of a deployed mission data set.

We hope this article has shown how important anomaly reporting is to the production of high quality MDS. If you have questions about the operation of a particular MDS, please provide CECOM or ARAT-TA with specifics as soon as you can. After all, the MDS is built for your protection and mission success.

Written by Mr. Pete McGrew, SRI International, ARAT-TA

Open source references:
(1) World Electronic Warfare Aircraft by Martin Streetly, Page 120
(2) Casta-2E1 Brochure, All Russian Research Institute of Radio Engineering
(3) Janes Radar and Electronic Warfare Systems 1994-1995, Page 109
(4) International Countermeasures Handbook 1978, Page 266
(5) International Countermeasures Handbook 1978, Page 202
(6) Janes Land-based Air Defence, 1999-2000, Page 105
(7) Crotale New Generation Brochure, Thomson-CSF, 03-95
(8) Giraffe Brochure, Ericsson Radar Electronics, 1993
(9) International Countermeasures Handbook 2000, Page 266
(10) International Countermeasures Handbook 1992, Page 194
(11) Flycatcher by R. Meller, Geneva
(12) Janes Land-Based Air Defence, 1991-1992, Page 285
(13) US National Spectrum Requirements, Projections and Trends, NTIA-94-31
(14) FM-24 Radio and Radar Reference Data, HQDA, December 1983, Page 8-2
(15) Introduction to Radar by Real Arsenault, Page 17
(16) Defense Electronics Handbook 1992, Page 183
(17) Periscope, USNI Military Database, 1998
(18) Janes Radar and Electronic Warfare Systems 1998-1999, Page 109
(19) International Defense Electronics Handbook 1992, page 199
(20) Sentinel Brochure, IEW&S, Redstone Arsenal
(21) Surface Warfare School Documents, Command Training Code 40, Combat Systems Engineering, slide #24
(22) WWW.FAS.ORG/MAN/DOD-1/SYS/SHIP/WEAPS/AN-SPS-67.htm
(23) AN/APN-241 Brochure, Northrop Grumman, BR-053-GSM-0896, Page 6
(24) Longbow: an extended arm for the attack helicopter by W. H. Campbell, Martin Marietta Corp.

Technical Talk

The Art and Science of Jamming

The U.S. Army employs a comprehensive approach to aircraft survivability. The Aviation Survivability Equipment (ASE) Philosophy taught at the EW Officer course at Ft. Rucker, AL consists of a sequence of defenses for Army aircraft. Each step of the sequence is designed to protect the aircraft once the previous step fails. The steps in the sequence are: threat avoidance/tactical approaches, aircraft signature reduction, threat warning, jamming and decoying the threat, and aircraft hardening against weapons effects. This approach has proven itself effective in the most hostile air defense environments. However, technical evolution has all but compromised a key step in the sequence. Improvements in air defense radar technology have made successfully jamming RF threats increasingly difficult. ***(cont. next page)***

Jamming (cont.)

The advent of integrated circuitry (IC) profoundly affected the EW environment. The miniaturization of components and rapidly increasing speed of microprocessors gave radar designers the tools to produce air defenses capable of complex processing of radar signal returns. IC technology resulted in the appearance of Doppler processing, phased array antennas, and adaptive pulse frequency modulation (PFM). These innovations, along with monopulse target tracking, have led to a new generation of air defense systems that are practically impossible to jam with current techniques. There is more bad news for the EW community, though. The innovations in software design have been incorporated into air defense systems as well. Software-controlled radars can change their operating mode in response to target maneuvers and countermeasures in a matter of milliseconds, far faster than the most experienced gunners ever could. Software control also reduces the problem of inexperienced gunners. Highly automated air defense systems work equally as well in Third World countries as they do for the countries that designed them. The new generation of air defense systems, with their digital processing technology, is more lethal and more difficult for the EW community to counter.

What is it about the new technology that makes jamming so difficult? To answer that question, we must examine what the jamming attempts to do and what techniques are used. Jamming threat system radars is primarily accomplished by making the radar think its target is at a location in the sky where it actually is not. The goal is to make the radar point the gun or the missile away from the aircraft. This type of jamming is known as deception jamming and also as repeater jamming. The method used to deceive the radar is to transmit a high powered, slightly altered version of the signal the radar transmitted to the target. The high power of the jamming signal will force the radar to reduce its receiver sensitivity, in essence, to "turn down the volume". By doing this, the radar cannot hear its own signal anymore because it has much less power. At this point, the radar is listening only to the jammer. The jammer is free to feed the radar false information about the target's range, speed, azimuth and elevation. At a critical moment, the jammer will stop transmitting, causing the radar to completely lose track of the target. Now we reach the key to successful jamming: to produce the slightly altered signal to fool the radar, the jammer must know what the radar signal looks like and what it will look like in the future. To jam the radar, its signal must be predictable. Here is where we encounter the problem with the new generation air defenses. The new technologies incorporated into their radars makes their signals less predictable. Let's examine each technology and its effect on the radar signal.

Monopulse Tracking

Radars must keep the antenna pointed at the target to maintain the track. Much older radar did this by moving the radar beam around the target in a circular pattern and would compare the return power level vs. antenna position to correct the pointing angle. The direction with the greatest power is where the target lies and is the direction the antenna must move. These radars were easy to jam by manipulating the power levels. Monopulse tracking enabled the radar to correct the pointing angle with each individual pulse. The antenna is designed to break the radar beam into several narrow beams. The returns of the beams are analyzed simultaneously to determine the antenna pointing correction required. This technology eliminated some of the most effective jamming techniques that were collectively known as Angle Walk Offs and Angle-On jamming.

In the next issue of the “A/IEW Bulletin”, we will examine Pulse Doppler, Adaptive PFM and Phased Array Antennas.

Written by Mr. Carl Brunner, SRI International, ARAT-TA

SEC's GUARDRAIL Branch (cont. from Page 3)

Technical

- Leveraging lessons learned from prior GR systems' development and support actions;
- Maintaining and enhancing experience, expertise, a 'hands-on' competency, and a 'corporate' knowledge-base, for achieving software system development, fielding, support, and Software Trouble Report (STR) rework and resolution;
- Accomplishing proof-of-concept via studies, prototypes, test beds and Computer Engineering Labs (CELs);
- Acquiring expertise in new technologies, Website solutions and open architectures;
- Developing Commercial Off-The-Shelf (COTS)-based solutions;
- Mitigating for Y2K and Joint Technical Architecture-Army (JTA-A) compliance.

These types of activities have been applied successfully for years in achieving beneficial, real-time results in support of SEC customer PMs and their systems. Some noteworthy accomplishments are:

- Integrating of JTA-A compliant Local Area Network (LAN) architectures into the legacy systems, providing opportunities for expanded reuse;
- Improving system reliability by replacing obsolete display terminals with PC-based platforms;
- Upgrading GR System 1 to include the Communications High Accuracy Airborne Location System (CHAALS) Remote Relay capability;
- Upgrading GR System 4 to include the Communications High Accuracy Location Subsystem (CHALS) Remote Data Link (RDL) processor.

Written from the perspective of the GUARDRAIL Team, Part II of this article will provide insight into the unique support the GR organization is providing to the ACS (Aerial Common Sensor) Program (the future GUARDRAIL). The ACS areas that will be explored are:

- Competing-Primes Contract Solicitation;
- Modeling and Simulation;
- Object-Oriented (OO) Analysis;
- Joint Development (Technology Insertion and Sharing);
- Warfighter Needs Analysis.

In Part II of this article, we will also examine some areas that can evolve into future capabilities for SEC in supporting a wide range of PM customers' systems and their software needs, should such opportunities arise.

Written by Mr. Ray Santiago and Mr. Larry Lashine, CECOM SEC, and Ms. Brenda Klafter, ILEX Systems

Notes to the Field

The New Face in Secure Telephone Equipment

As of 1 January 2000, the familiar Secure Telephone Unit-III (STU-III) is no longer available for purchase. The reason for this is that a new device is replacing the STU-III, called the "Secure Terminal Equipment" or STE. This article provides information on ordering both a STE and the required KOV-14 cryptographic cards.

As stated on the Government's official STE website (http://ste.securephone.net), "STEs are the next generation of secure voice and data equipment for advanced digital communications networks, such as Integrated Services Digital Network (ISDN). The STE consists of a host terminal and a removable security core. The host terminal provides the application hardware and software. The security core is a FORTEZZA^{TM} PLUS^{KRYPTON} cryptographic card, which provides all the encryption and other security services.

The first STE products are capable of connecting to both Integrated Services Digital Network (ISDN) and analog Public Switched Telephone Network (PSTN) telephone lines. ISDN provides the speed and high quality digital connections that enable toll quality secure voice (32 kbps vs. 4.8 kbps), faster data rates (up to 128 kbps vs. 9.6 kbps), secure three party conferences and STU-III compatible modes. When connected to PSTN, STEs will emulate STU-IIIs (2.4-4.8 kbps voice, 2.4-9.6 kbps secure data). STEs will be software upgradeable to provide future enhancements to fielded products."

STEs have National Stock Numbers (NSN) (see below) and are considered Common Table of Allowance (CTA) 50-909 items. Commanders can authorize any number of secure phones, based upon mission requirements, as long as the unit can afford to purchase them (using Operation and Maintenance, Army [OMA] funds). STEs can be ordered by submitting a DD Form 448, Military Interdepartmental Purchase Request (MIPR), through S4/Supply channels, to the Army POC that appears later in this article.

Currently, there are three variations of the STE available for purchase:

- Office (voice/data) STE (ISDN/PSTN), NSN 5810-01-459-6441, $3250
- Data-only STE (IDSN/PSTN), NSN 5810-01-457-0298, $2930
- Tactical STE, NSN 5810-01-459-6438, $3725. There are additional items available, which can be included on the same MIPR as the phone. Note: you must order a KOV-14 cryptographic card as a minimum to be able to use the phone in a secure mode.
- Fortezza^{TM} Plus ^{KRYPTON} (KOV-14) card, $255 (must also fill out a "STE Key Order Request" COMSEC form)
- Portable Uninterruptible Power (PUP) Supply, $2814 (for tactical use – connects a STE [not included] to a battery power supply)
- Tactical STE with PUP, $6539 *(cont. next page)*
- STE Push-to-Talk Handset, $75

Secure Telephone Equipment (cont.)

- STE One Year Warranty Extension (All Models), $120 (STEs come with a three year warranty – this would make it four years)
- STE Five Year Warranty Conversion (2 Additional Years of Warranty), $230

To order a STE and/or additional accessories, submit a MIPR, through S4/Supply channels, to:

Commander, USACCSLA
ATTN: SELCL-IA-A
Fort Huachuca, AZ 85613-7090

The MIPR must include the following information, as a minimum: Unit Department of Defense Activity Address Code (DODAAC), Unit Communications Security (COMSEC) account number, full shipping location mailing address specifying building number and/or room number, and Point of Contact (POC) name, both DSN and Commercial Phone Numbers and Fax Numbers, and unclassified (Internet) email address. MIPRs must be mailed to the above address, however, advanced copies may be faxed (with a STE Key Order Request form-see below) to the US Army CECOM-Communications Security Logistics Activity (CCSLA) at DSN (312) 879-6143, CML (520) 538-6143, ATTN: Ms. Nancy Calderon. Ms. Calderon may be reached at DSN (312) 879-8338, CML (520) 538-8338, email: calderonn@csla.army.mil. (Note: Although a National Security Agency [NSA] address is shown on the Government's STE website, do not send your MIPR to that address; use the CCSLA information given in this document. They will forward your request, as NSA will reject your MIPR if it does not come from the Army Service POC.)

Ensure that the STE product(s) you order have both the Integrated Services Digital Network (ISDN) and the analog Public Switched Telephone Network (PSTN) capability. When connected to the PSTN, STEs are interoperable with STU-IIIs (2.4 - 4.8 kbps for voice and 2.4 - 9.6 kbps for data).

When ordering a STE, include all required items on the same MIPR, including KOV-14 crypto-cards and optional warranty extensions. In addition, a "STE Key Order Request" form must accompany the MIPR to have the appropriate keymat loaded onto the KOV-14. Otherwise, the KOV-14 cards will not work with your STE. Your COMSEC Officer/Custodian should have the "STE Key Order Request" forms; otherwise, use the one enclosed in this bulletin. The "STE Key Order Request" form must be coordinated with your COMSEC Officer/ Custodian to ensure that it is filled out correctly.

Note: The MIPR and "STE Key Order Request" forms must be faxed/mailed to the CCSLA together. The STE manufacturer will ship the unit to you; the KOV-14 crypto-card will be sent to your COMSEC Officer from NSA's Key Management Center. The two devices will probably not arrive at the same time.

Should you rush out and purchase a STE if you already have a STU-III? Not necessarily. Your STU-III will still provide you access to ARAT services such as the MSEWBBS and the ARAT Web. Since each unit's mission and requirements are different, your Signal Officer can assist you in determining which STE would be best suited for use with your unit's organic tactical signal equipment.

Written by Mr. Andrew Lombardo, ILEX Systems

For Your Information

Coming Events!

Event	Location	Date(s)
Armed Forces Day	*Fort Monmouth, NJ*	*20 May 2000*
3rd International EW Conference and Exposition	*Zurich, Switzerland*	*21-24 May 2000*
AFCEA Technet	*Washington, D.C.*	*20-22 June 2000*
37th Annual AOC International Symposium & Convention	*Las Vegas, NV*	*1-5 October 2000*

-

Now Available on the Web

All 18 previous issues of the "ARAT Bulletin" (now known as the "A/IEW Bulletin") are now available on the ARAT web site. The issues are available in HTML format for on-line viewing, as well as in PDF and MS Word 97 format for viewing and downloading.

Future issues will also be posted on the site and in the same format. You are encouraged to download any issue (or issues) for local reproduction and distribution within your agency. The ARAT web site can be accessed at http://arat.iew.sed.monmouth army.mil/, or from a link on the A/IEW web site at http://www.iew.sed.monmouth.army.mil/.

Help Us Help You

If you are moving, have moved, or your address is listed incorrectly on the mailing envelope, please call Ms. Tara Hurden at (732) 532-5319, DSN 992-5319; or email at hurden@mail1.monmouth.army.mil with the correct address. Many Bulletins are returned for incorrect addresses and unknown addressees. We'd like to reduce the amount of returned mail and ensure that all of our customers receive the latest issue of the "A/IEW Bulletin". Thank you for your support.

ARAT Rapid Reprogramming Communications Infrastructure Laboratory (R^2CIL)

Telephone:
#1 (732) 532-9395
DSN: 992-9395
#2 (732) 532-9392
DSN: 992-9392
#3 (732) 532-1859
DSN: 992-1859
#4 (732) 532-5319
DSN: 992-5319 -or-*
(732) 530-7766 ext.: 318 or 324**
** Answering machine/voice mail option available at this number for after-hour messages*

Email:
Unclassified:
arat@arat.iew.sed.monmouth.army.mil
SIPRNET:
webmaster@arat.army.smil.mil

ATTENTION ELECTRONIC WARFARE OFFICERS!

Electronic Warfare Officers requiring Memory Loader/Verifier (MLV) reprogramming kits should contact either Ms. Fanny Leung-Ng (DSN: 312-992-1859/ CML: 732-532-1859) (leungf@mail1.monmouth.army.mil) or Ms. Tara Hurden (DSN: 312-992-5319/ CML: 732-532-5319) (hurden@mail1.monmouth.army.mil) or fax your requests to DSN: 312-992-8287/5238 or CML: (732) 532-8287/5238.

For Your Information

The A/IEW Community Key Points of Contact

Agency	Name/e-mail	Comm/DSN	Fax Number
Chief, A/IEW Division	Dr. Ihor Hapij hapij@mail1.monmouth.army.mil	(732) 532-8199 DSN 992-8199	(732) 532-8287 DSN 992-8287
Deputy Chief, A/IEW Division	Mr. Joseph Ingrao ingrao@mail1.monmouth.army.mil	(732) 532-1337 DSN 992-1337	(732) 532-5238 DSN 992-5238
Avionics Branch	Mr. Edward Wuysick wuyscik@mail1.monmouth.army.mil	(732) 427-3924 DSN 997-3924	(732) 427-3923 DSN 997-3923
Electronic Combat Branch ARAT-SE (CECOM)	Mr. Gary Clerie clerie@mail1.monmouth.army.mil	(732) 532-0065 DSN 992-0065	(732) 532-5238 DSN 992-5238
GUARDRAIL Branch	Mr. Raymond Santiago santiago@mail1.monmouth.army.mil	(732) 532-1420 DSN 992-1420	(732) 532-8287 DSN 992-8287
Intelligence Fusion Branch	Mr. William Walker walker@huachuca-emh27.army.mil	(520) 538-6188 DSN 879-6188	(520) 538-7673 DSN 879-7673
SIGINT Branch	Mr. Robert Hart hartR@mail1.monmouth.army.mil	(732) 532-6253 DSN 992-6253	(732) 532-8287 DSN 992-8287
Sensors Branch	Mr. Frank Toth toth@mail1.monmouth.army.mil	(732) 532-8353 DSN 992-8353	(732) 532-8287 DSN 992-8287
ARAT-TA (Eglin AFB)	Mr. Norman Svarrer svarrer@eglin.af.mil	(850) 882-8899 DSN 872-8899	(850) 882-9609 (C) -4268 (U) DSN 872-9609 (C) -4268 (U)
ARAT-TA (Kelly AFB)	SSG Edward L. Wiggins elwiggi@afwic.osis.gov	(210) 977-2021 DSN 969-2021	(210) 977-2145 DSN 969-2021
ARAT-SC (Fort Rucker)	Mr. George Hall hallg@rucker.army.mil	DSN 558-9334	DSN 558-1165

The A/IEW Bulletin Staff	
Editor-In-Chief Mr. Joseph Ingrao, A/IEW Division **Editors** Mr. Joseph Skarbowski, Ilex Systems, Inc. **Distribution Manager** Ms. Tara Hurden, SRI, International.	Send comments, changes of address, and articles to: U.S. Army CECOM Software Engineering Center ATTN: AMSEL-SE-WS-AI Fort Monmouth, NJ 07712 FAX: 992-5238 (DSN); 732-532-5238 (Commercial)